UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

1105 Park Glen Place
Durham, North Carolina

Case No. 1:21MJ49-1

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

1105 Park Glen Place, Durham, North Carolina, further described in Attachment A, incorporated by reference.

located in the Midde District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment A1, incorporated by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
26 U.S.C. §§ 7201, 7203 18 U.S.C. §§1956(a)(3)(B), 1960	§7201 (Attempt to evade or defeat tax); §7203 (Willful failure to file return, supply information, or pay tax); §1956(a)(3)(B) (money laundering concealment); §1960 (unlicensed money service businesses)

The application is based on these facts:

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Robert Nordlander
Applicant's signature

Robert Nordlander, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 02/08/2021 11:12am

Judge's signature

City and state: Durham, North Carolina

Joe L. Webster, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Robert Nordlander, being first duly sworn, do hereby state the following:

AFFIANT'S EXPERIENCE

1. Your affiant, Robert Nordlander, is a special agent with the Internal Revenue Service, Criminal Investigation (IRS-CI) in Greensboro, North Carolina. Your affiant is a law enforcement officer of the United States. Accordingly, your affiant is authorized to conduct investigations and make arrests for violations of the Internal Revenue Code and other Title 18 and 31 violations.

2. Your affiant has been a special agent with the IRS-CI for over 20 years. Your affiant received an undergraduate degree in accounting, a graduate degree in business administration, and a CPA license. Your affiant's duties include investigations of possible criminal violations of the Internal Revenue laws (Title 26, United States Code (U.S.C.)) and other criminal offenses (Title 18 and Title 31, U.S.C.).

3. Your affiant graduated from the Criminal Investigator Training Program and the IRS-CI Special Agent Investigative Training program at the Federal Law Enforcement Training Center. During this period, your affiant received extensive training in law enforcement and financial investigative techniques and procedures.

4. As a special agent with IRS-CI, your affiant has participated in and conducted criminal investigations of violations of Title 26, U.S.C., Sections

7201 (attempt to evade or defeat a tax) and 7203 (willful failure to file return, supply information, or pay tax), and various Title 18 violations. Your affiant has also participated in multiple search warrants involving violations of the before-mentioned crimes.

GROUNDS FOR SEARCH WARRANT

5. Based on the facts set forth in this Affidavit, your affiant believes there is probable cause that Jayton Gill (Gill), doing business as Bits of 8 LLC (Bof8), has committed violations of Title 26, U.S.C. Sections 7201 (attempt to evade or defeat a tax) and 7203 (willful failure to file return, supply information, or pay tax), Title 18 U.S.C. Section 1956(a)(3)(B) (money laundering concealment), and Title 18 U.S.C. Section 1960 (unlicensed money service businesses). Your affiant seeks a warrant for evidence and fruits of criminal violations of Title 26, U.S.C. Sections 7201 and 7203, and Title 18 U.S.C. Sections 1956(a)(3)(B) and 1960, as well as property designed for use, intended for use, or used in committing those offenses.

6. Further, your affiant believes there is probable cause that evidence and fruits of the crimes described above (as well as property designed for use, intended for use, or used in committing those offenses) is located at the personal residence of Jayton Gill at 1105 Park Glen Place, Durham, North Carolina ("Gill's Residence"), Gill's 2012 Ford Fusion with North Carolina tag number DEP7185, and on Gill's person. Your affiant makes this Affidavit in support of the issuance of a search warrant for Gill's Residence, (more particularly described in Attachment A), Gill's vehicle (more particularly described in Attachment B), and on his person (more particularly described in Attachment C).

7. The residence of Jayton Gill described in Attachment A is located in Durham County, in the Middle Judicial District of North Carolina. The vehicle described in Attachment B is also located in the same district.

8. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This Affidavit is not all inclusive of the facts known to your affiant. Your affiant has relied on financial documents, witness testimony, and other evidence that are presented in this Affidavit.

AFFIANT'S KNOWLEDGE

9. From your affiant's training and experience, your affiant knows the following:

   a. Businesses typically store their business records at their business location. A business location can also be in a personal residence. Such records maintained by a business would include bank statements, check stubs, checks, deposit slips, payment records, correspondence with customers and others, emails, faxes, letterheads, client files, employee files, etc.

   b. When a business relocates, the records follow the business and typically are stored at the new location. If a person operates a business in his residence and moves to another residence, the person will take his personal and business records with him to the new residence.

c. Self-employed individuals in certain industries can operate their business from their personal residence. If a self-employed individual does operate his business apart from his residence, it is common that business records will be maintained at both the residence and business location.

d. An individual's personal bank records and financial transactions are typically kept at their residence. Such records include bank statements, insurance documents, mortgage documents, personal tax returns, charitable contributions, real estate records, vehicle records, etc.

e. Due to COVID-19 travel restrictions and occupancy restrictions, many individuals are working at their residence. Since March of 2020, more workers and business owners are working from their residence as part of a nationwide trend in teleworking.

f. When a business is incorporated as a Limited Liability Corporation (LLC), the IRS allows the LLC discretion on how it is treated for tax purposes. If the LLC has only one member as an individual person, then it is considered a sole member LLC. The income and expenses can be filed on a corporate tax return or as a sole proprietorship on the individual's personal income tax return. If no corporate tax return is filed, then the business operations should be reported as a sole proprietorship on a Schedule C of the individual's income tax return; Whether the LLC is a sole proprietorship or corporation, it is required to file its business operations with the IRS. The IRS uses this

information to assess the proper income taxes and to ensure that benefits such as wages, dividends, etc. can be traced to an individual's personal income tax returns. When businesses fail to file the proper records with the IRS, the IRS has insufficient knowledge of individual taxpayers' income.

g. Individuals are required to file personal income tax returns (Forms 1040) to the IRS if their gross income exceeds the filing requirement. For the tax years 2015 to 2019, gross income exceeding these amounts require a personal income tax return to be filed:

Year	Single
2015	$10,300
2016	$10,350
2017	$10,400
2018	$12,000
2019	$12,200

h. Businesses are required to file corporate tax returns to the IRS, even if gross receipts are nonexistent.

i. Individuals who hide their income from the IRS will typically not deposit all their cash receipts into a financial institution. This activity hampers the government's efforts to accurately calculate a taxpayer's true income and true tax liability. The cash is then used for other purposes, which cannot be traced from normal business transactions.

j. Individuals who attempt to hide their income from the IRS or engage in money laundering purchase debit cards that can be "loaded" or

credited with cash deposits. The card can then be used to make purchases or transfer funds to another account. Because these cards are not tied to a typical financial account such as checking or savings account, the source of deposits credited to this card and subsequent purchases on the card are hard to detect by law enforcement and government taxing authorities. Because a traditional bank account is not used, the cardholder can remain anonymous or allow another individual to use the card. These cards can be found on a person, in a person's wallet, purse, vehicle, or residence.

k. Individuals who engage in money laundering typically allow deposits into their bank accounts from others. These accountholders will utilize bank accounts that allow deposits from various bank branches around the United States or abroad internationally. An anonymous person can make a deposit into an accountholder's account at a local bank branch. This deposit will be immediately credited to the accountholder. The accountholder will then transfer funds per the customer's request, or the accountholder will transfer value through another means to the customer. This allows the customer to stay anonymous as well as facilitate a secure banking transaction. For example, if a drug dealer in North Carolina needs to pay his supplier in California, the dealer can directly deposit cash into the supplier's bank account in North Carolina. This allows the supplier to access the account either in California or another location.

l. CO-OP Shared Branch network is a national network of credit unions from all over the United States that allows members to perform financial transactions at another credit union. Unlike national brand

banks, many credit unions are local or regional, and do not have branches nationwide. Through this shared network, participating credit unions can serve members in various geographical locations, such as allowing deposits into bank accounts.

m. Individuals who try to hide their income and assets from the IRS often do not file personal income tax returns. Personal income tax returns are due on the 15th after the third month of the fiscal or calendar year. For most taxpayers, personal income tax returns are due on April 15th. Extensions to file personal returns can be requested, which extends the due date another six months, which in most cases becomes October 15th. Not filing a personal income tax return on time is a violation of Title 26, U.S.C. Section 7203 (failure to file a tax return).

n. Individuals who try to hide their income and assets from the IRS often use nominee entities, such as a corporation or trust, to serve as a conduit to pay their personal living expenses. Personal living expenses are disbursed from bank accounts of nominee entities to hide their true purpose. When the business entities do not file their annual tax return, the IRS must 1) determine the source of the taxpayer's personal living expenses, and 2) separate the legitimate business expenses and personal living expenses to calculate a tax due. It is not uncommon for personal living expenses to be concealed as a business expense so the taxpayer can avoid paying federal income taxes on that income.

o. Individuals who try to hide their true income from the IRS also deal in a cash lifestyle. Because the source and disposition of cash is not

traceable like a check, cash can be used to purchase assets, pay for personal living expenses, or facilitate other transactions.

p. Because of the prevalence of cell phones, computers, and the use of the internet in society, many transactions, texts, and emails are used on personal computers, laptop computers, tablets, and smart phones. These digital devices not only are used in the crime, but often store evidence of these crimes. Such electronic devices are owned by individuals and businesses and are stored in their residence, business, vehicle and on their person.

q. Cryptocurrency is virtual currency that uses cryptography to ensure that unauthorized users cannot access the funds. Bitcoin is the most common cryptocurrency. Bitcoin addresses (similar to bank account numbers) are recorded in a blockchain ledger. This ledger is maintained by multiple independent decentralized computers connected to the internet that are operating Bitcoin software. The Bitcoin software is open source to the public, meaning anyone can analyze it and use it. Through various checks and balances, the ledger is updated approximately every 10 minutes.

r. Accessing Bitcoin requires two separate keys: a private key and public key. The public key is listed on the blockchain ledger as the Bitcoin address. This address is unique (just like a routing number and bank account number is unique). The public key is also like a home address. The private key is a password, like a key to the front door of the home address. Both keys are needed to gain access to the Bitcoins attributed to that address (home address). Since Bitcoin addresses do

not reveal ownership (like a bank statement does with an account number), various software is available to try to determine the true owner by using logic and scientific guesses.

s. To conduct a payment, the receiving Bitcoin address only needs to be disclosed to the sender to receive Bitcoin. Only the sender of Bitcoin needs their public key and private key to conduct the transaction. Like a bank account, the Bitcoin address is all that is needed to receive a deposit; however, to withdraw funds, the bank account number and password are required. The blockchain ledger is how Bitcoin transactions are recorded.

t. For ease of use, Bitcoin wallets are created. These wallets are like a wallet that can be carried if you have more than a single unit of currency. The wallet can be virtual or physical, both of which contain the public key and private key of your Bitcoins. Wallets come in various forms: desktop, laptop, smart phone, and other ways to store electronic data.

u. Individuals who engage in exchanging cryptocurrency for cash or vice versa will charge a fee. The industry standard for exchanges is 5% to 7%. Because of the anonymity of Bitcoin transactions, many illegal activities used Bitcoin as the conduit to conduct business transactions. Such illegal activities include terrorism financing, child exploitation, murder for hire, illegal drug trafficking, identity theft, computer intrusion, ransomware, etc. These activities can be purchased and sold using dark markets, such as Silk Road, Empire, Dream Market, etc.

v. Title 26, U.S.C. Section 7201 states that the willful attempt to evade or defeat the *assessment* of a tax is a violation with punishment up to five years. *Elements of the offense:* [1] An attempt to evade or defeat a tax or the payment of a tax; [2] An additional tax due and owing; and [3] Willfulness.

w. Title 26, U.S.C. Section 7203 states that "failure to file proper tax returns" is a violation with punishment up to one year. *Elements of the offense:* [1] Person required by law to file a return for the taxable period [I.R.C. § 6012]; [2] A failure to file a return at the time required by law [I.R.C. § 6072]; and, [3] Willfulness.

x. Title 18, U.S.C. Section 1956 (a)(3)(B) states that "whoever with the intent to conceal or disguise the nature, location, source, ownership, or control of property believed to be the proceeds of specified unlawful activity, conducts or attempts to conduct a financial transaction involving property represented to be the proceeds of specified unlawful activity, shall be fined under this title or imprisoned for not more than 20 years, or both. *Elements of the offense:* [1] Person knowingly conducts or attempts to conduct a financial transaction; [2] The financial transaction or attempted financial transaction must involve property represented to be the proceeds of specified unlawful activity by a law enforcement officer authorized to investigate or prosecute violations of 18 U.S.C. Section 1956, and [3] with the intent to conceal or disguise the nature, location, source, ownership, or control or property believed to be the proceeds of specified unlawful activity.

y. Title 18, U.S.C. Section 1960 states that "whoever knowingly, conducts, controls, manages, supervises, directs or owns all or part of an unlicensed money transmitting business, shall be fined in accordance with this title or imprisoned not more than 5 years, or both. *Elements of the offense:* [1] Person conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business; [2] Person acted knowingly. An "unlicensed money transmitting business" is a money transmitting business that affects interstate or foreign commerce in any manner or degree and (1) is operated without a required money transmitting license; (2) fails to comply with the applicable money transmitting business registration requirements under Title 31; or (3) otherwise involves the transportation or transmission of funds that are known to be derived from a criminal offense or are intended to support unlawful activity.

z. "Money transmitting businesses" and "money services businesses" (MSB) are terms used by Title 31 and the regulations implementing the registration requirements, respectively. These terms should be understood to encompass the same array of businesses. Currency dealers or exchangers, and money transmitters are considered MSBs, as are entities that transmit virtual currencies such as Bitcoin to another person or location for its customers.[1]

aa. Under the Bank Secrecy Act, a MSB is subject to the federal anti-money laundering regulations of the Financial Crimes Enforcement Network (FinCEN). In addition, the IRS has the authority to examine

[1] *See, e.g., United States v. Murgio*, 209 F.Supp.3d 698, 711 (S.D.N.Y. 2016).

MSBs with respect to their compliance with FinCEN's anti-money laundering regulations.

bb. A "money transmitter" is a type of MSB that is regulated by FinCEN. FinCEN defines the term "money transmitter" as "a person that provides money transmission services" or "any other person engaged in the transfer of funds." 31 C.F.R. § 1010.100(ff)(5)(i). FinCEN defines "money transmission services" as "the acceptance of currency, funds, or other value that substitutes for currency from one person *and* the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means." 31 C.F.R. § 1010.100(ff)(5)(i)(A).

cc. On March 18, 2013, FinCEN issued regulatory guidance highlighting that under existing regulations, an administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN's regulations, unless a limitation to or exemption from the definition applies to the person." "Exchanger" was defined as "a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency." *See* FIN-2013-G001, *available at www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf*

BACKGROUND OF INVESTIGATION

10. Jayton Gill was identified as an individual who was operating an unlicensed MSB. He advertised his services to exchange Bitcoin and

cash on the website Localbitcoins.com and Paxful,com under the online moniker "Rishodi." Bitrated.com identified Gill as Rishodi, which included a photo of Gill. Rishodi's Youtube channel shows Gill in its videos.

11. Gill's Localbitcoins.com profile describes himself as professional Bitcoin trader since 2013 with over 3,000 trades with over 2,800 different partners and a trade volume of over 500 Bitcoins. His Paxful profile page claims he has advertised his MSB services since 2016 and has conducted over 4,000 trades with over 2,700 trade partners and with a trade volume of between 300 to 1,000 BTC (between $2.9MM to $9MM based on today's nominal USD price of Bitcoin). His Paxful profile was active showing services as late as November 20, 2020. Based on the comments of these websites, his services include sending cash by mail, exchanging face to face, placing funds on gift cards, and depositing cash into bank accounts.

12. Your affiant has not found any evidence that Gill or Bof8 is a licensed MSB with the Financial Crimes Enforcement Network (FinCen), at the United States Department of Treasury. Neither Gill nor Bof8 is found in FinCen's search directory of licensed MSBs. Neither is Gill nor Bof8 registered with the North Carolina Commissioner of Banks, which would be required by North Carolina state law to operate as a MSB.

FBI Undercover Operation

13. In an approved undercover operation, a FBI undercover agent (UCA) engaged GILL to exchange cash for Bitcoin through one of Gill's online

advertisements. Gill used the online moniker "Rishodi". Gill and the UCA communicated through texts and Signal App, which is an encrypted texting application. Gill's cellphone number during the UC operation was 540-921-7727. Gill stated to the UCA that he uses various encrypted messaging apps, such as Signal, Wicker, and Telegram. Gill used his phone in every transaction with the UCA. The UCA never saw Gill with multiple phones. The UCA and Gill met on seven occasions, in which the UCA gave Gill a total of $83,000 in cash in exchange for Bitcoin. Gill took a fee for each transaction. The following table shows the date, time, and location where they met, and the amount of cash exchanged for Bitcoin.

Date	Location	Amount
May 28, 2019	Starbucks 6813 Fayetteville Road, Durham, NC	$3,000
June 13, 2019	Starbucks 3711 Elmsley Street, Ste 108, Greensboro, NC	$5,000
August 13, 2019	Starbucks 3711 Elmsley Street, Ste 108, Greensboro, NC	$5,000
November 8, 2019	Starbucks 3711 Elmsley Street, Ste 108, Greensboro, NC	$10,000
February 27, 2020	Walmart 1116 Crossroads Dr, Statesville, NC	$20,000
May 7, 2020	Courtyard Marriott 222 West W.T. Harris Blvd, Charlotte, NC	$20,000
August 27, 2020	Near Planet Fitness 1720 Guess Road, Durham, NC	$20,000

14. Gill drove his vehicle, a 2012 Ford Fusion, as described in Attachment B, to each of the transactions. North Carolina Department of Motor Vehicle records show that Gill owns a 2012 Ford Fusion (VIN

3FADP0L37CR242765) with North Carolina tag number DEP7195, registered at 1105 Park Glen Place, Durham, North Carolina. His North Carolina driver's license also identifies 1105 Park Glen Place as his personal residence.

15. For the meeting on May 7, 2020 between Gill and the FBI UCA, the FBI UCA gave Gill a brown paper bag containing $20,000 in cash. Gill used a money counter to count the cash. After counting the funds, Gill told the UCA that he could exchange up to $50,000 in cash. The UCA told Gill that the cash came from narcotics sales proceeds and asked Gill if he was ok with the source of the funds. Gill was not concerned about the source coming from the illegal source. Gill transferred the Bitcoin to the UCA's account.

16. As part of the undercover operation, surveillance teams were used to provide cover for the UCA and to positively identify Gill and his activities. On or about October 23, 2020, Gill contacted the UCA via the Signal app stating that he was dropping his sales commission for transactions from 7% to 5%.

Surveillance on Gill to and from his residence

17. On August 27, 2020, the surveillance team saw Gill leave his residence at 1105 Park Glen Place, Durham, North Carolina. Gill was driving his 2012 Ford Fusion. Soon thereafter, Gill met the UCA at the parking lot near Planet Fitness, where the cash and Bitcoin exchange occurred. Gill was carrying a black bag, where he put his cash during the meeting.

18. After meeting the UCA, Gill went to another location (Starbucks, 5319 New Hope Commons Drive, Durham, North Carolina) where he met an unknown individual. Based on the surveillance team's experience, it appeared that Gill was conducting another business transaction. The unknown individual got into Gill's vehicle. They later exited their vehicle and went to an outdoor seating area at Starbucks. There the unknown individual used a laptop, which appeared to have a bar code on the screen, which is consistent with trading in Bitcoin.

19. After the second meeting, the surveillance team followed Gill to Coastal Federal Credit Union, located at 7103 NC Hwy 751, Durham, North Carolina. Gill was seen conducting business with the bank in the drive thru area. Gill is known to have active bank accounts at Coastal Federal Credit Union. Bank records show that he deposited $9,140 in cash in 16 separate transactions at the ATM machine into his personal bank account. After making his transactions, the surveillance team followed Gill back to his residence, where he was seen carrying the same black bag into his residence.

20. Based on the surveillance and your affiant's training and experience, your affiant has probable cause to believe that Gill is operating his unlicensed MSB from his personal residence, as described in Attachment A, and using his vehicle, as described in Attachment B.

21. On February 2, 2021, your affiant drove by Gill's personal residence, as described in Attachment A, around noon. Your affiant observed Gill's vehicle, as described in Attachment B, in the driveway.

Real Estate

22. In 2012, Gill purchased a residence at 3909 Ludgate Drive in Durham, North Carolina for approximately $94,000. He obtained a mortgage for the purchase. IRS records show that Gill was an employee of IBM in 2012 and 2013.

23. In 2018, he purchased another residence located at 1105 Park Glen Place in Durham, North Carolina for approximately $314,000, which is further described in Attachment A. No lien was recorded for this purchase. Bank records show a wire transfer to a real estate closing attorney for the full purchase price. As of November 29, 2020, courthouse records show that both houses are currently owned by Gill.

Business Records

24. According to the North Carolina Secretary of State's office, Gill incorporated Bof8 in the State of North Carolina in 2014. Gill used his personal address at that time located at 3909 Ludgate Drive, Durham, North Carolina as the business's registered address. On January 14, 2016, Bof8 was administratively dissolved by the State of North Carolina.

25. Records from the IRS show that Gill's former residence at 3909 Ludgate Drive was also the business address for Bof8 at the time of its inception.

26. Bank documents show that the business location of Bof8 was Gill's personal residence at 3909 Ludgate Drive up to 2017. Gill continued to use Bof8 even after it was dissolved by the State of North Carolina.

27. Your affiant has reviewed bank records of Gill and Bof8. Your affiant has not seen any evidence that Gill has a business office outside of his residence during the investigatory period.

Tax Returns

28. Your affiant reviewed the filing history of Jayton Gill (SSN ending 6192) for his U.S. Individual Income Tax Returns (Form 1040) for the years 2015 to 2019. The IRS has no record of Gill filing personal income tax returns since 2012. He has filed extensions for his Form 1040 for tax years 2015 to 2019, but all of these extensions have expired.

29. Gill made estimated payments for his Form 1040 for the years 2015 to 2019, in the following amounts:

Year	Amount
2015	$18,000
2016	$19,500
2017	$20,000
2018	$8,000
2019	$19,000

30. With these estimated payments, Gill filed Forms 4868 (Application for Automatic Extension of Time To File U.S. Individual Income Tax Return) for the years 2017 to 2019. In each of these years, he listed his address at 1105 Park Glen Place, Durham, North Carolina. For the tax years 2015 and 2016, Gill used 3909 Ludgate Drive, Durham, North Carolina as his address. Based on these records, your affiant believes that Gill's personal residence changed to 1105 Park Glen Place in 2018, which is consistent with time of Gill's purchase of 1105 Park Glen Place.

31. Depending on the type of income, these estimated payments would cover the federal tax liabilities of approximately $100,000 in annual gross income from 2015 to 2017 and 2019. For 2018, the estimated payments would cover $80,000 in annual gross income.

32. IRS records show that Bof8 (EIN ending 6776) was created in March of 2014 as a sole member LLC, with Gill as the sole member. The IRS has no record of Bof8 filing business tax returns.

33. IRS records show that Vortechs Computing (EIN ending 2776) was created as a sole proprietorship in September of 2019, with Gill as the point of contact. The address associated with this company is Gill's current residence at 1105 Park Glen Place, Durham, North Carolina.

34. The IRS has no record of employment such as Forms W-2 filed by an employer from 2015 to 2019 for Gill. Based on your affiant's experience with the facts known to date, Gill appears to be self-employed.

35. Since 2018, third party records sent to the IRS such as reporting interest income, mortgage interest, IRA balances, and CTRs filed on Gill, show Gill's address as 1105 Park Glen Place, Durham, North Carolina.

Bank Accounts

36. Your affiant also reviewed bank documents for Gill and Bof8. Not all known bank accounts have been thoroughly analyzed. However, for the purposes of this Affidavit, the following accounts have been identified with substantial activity:

Name	Bank	Account Ending	Year	Total Deposits
Jayton Gill	Coastal Federal Credit Union	4914-02	2015	32,466.79
			2016	79,519.86
			2017	161,178.30
			2018	524,423.95
			2019	109,960.21
Bits of 8 LLC	Coastal Federal Credit Union	1559-01	2015	281,484.61
			2016	118,623.83
			2017	346,041.65
Jayton Gill	Alliant	5099-40	2015	9,332.18
			2016	54,220.91
			2017	49,409.23
			2018	146,433.96
			2019	87,157.18
Jayton Gill	Alliant	5099-01	2015	1,451.04
			2016	3,682.67
			2017	94,545.60
			2018	83,938.71
			2019	89,590.21

Your affiant reviewed the disbursements in these accounts. The disbursements appear to consist of both business and personal living expenses. The Bof8 account closed in November 2017.

Some deposits into the accounts listed above are transfers between accounts. The next paragraph describes in more detail the characteristics of the deposits that are not transfers between accounts.

37. Based on the bank accounts listed in the previous paragraph, the following source of deposits (that are not transfer between accounts) was compiled:

Source	2015	2016	2017	2018	2019	Total
Amazon	$244,799.01					$244,799.01
Cash	$31,227.00	$63,481.00	$60,001.00	$27,660.00	$16,895.00	$190,599.00
Cursell			$100,000.00			$100,000.00
Hashmaster				$50,000.00		$50,000.00
Gemini				$403,911.07		$403,911.07

Unknown	$29,674.53	$19,141.47	$289,742.39	$9,995.01	$93,912.76	$442,466.16

Based on your affiant's training and experience (See paragraph 9(g) in affiant's knowledge) from the deposits listed above, Gill and Bof8 would be required to file income tax returns. Records show that Gill sold Bitcoin mining equipment through Amazon. Gemini is a cryptocurrency exchange. Hashmaster is a Bitcoin mining company which helps maintain Bitcoin blockchain. The business purpose of Cursell is unknown.

Of the unknown deposits, many of the deposits were made outside the Durham, North Carolina area where Gill resides. Deposits came from Florida, California, Oklahoma, Indiana, Colorado, Louisiana, South Carolina, Pennsylvania, Idaho, Wisconsin, Ohio, Tennessee, Virginia, Texas, New Jersey, Illinois, Alabama, Minnesota, Michigan, Nebraska, and Washington. The following chart shows that most of the unknown deposits were deposits from other locations, using the Shared Branch network. (See paragraph 9(l) in affiant's knowledge). This chart shows substantial amounts of deposits were being made into Gill's accounts at shared branch locations around the United States.

Source	2015	2016	2017	2018	2019
Unknown	$29,674.53	$19,141.47	$289,742.39	$9,995.01	$93,912.76
From Shared Branch Network	$1,202.00	$17,791.47	$264,505.15		$93,063.00
Percentage of Shared Branch Network Deposits out of Total Unknown Deposits	4%	93%	92%	0%	99%

38. From 2018 to current, bank statements from various financial institutions show Gill's address as 1105 Park Glen Place, Durham, North Carolina.

Other Discovered Financial Connections

39. Records from Bitstamp, a cryptocurrency exchange, show that Gill sold the following amounts of Bitcoin for the year 2015:

Month	Amount
January	$15,297.68
February	$30,545.19
March	$15,582.78
April	$31,847.53
May	$32,526.56
June	$29,983.11
July	$36,088.34
August	$8,070.98
September	$18,202.83
October	$20,907.70
November	$44,749.99
December	$28,735.77
Total	$312,538.46

40. Bitstamp conducted an analysis of Gill's Bitcoin transactions from his account. Bitstamp stated that 18% of Bitcoins that Gill withdrew from his Bitstamp account were sent directly Bitcoin addresses that are connected to dark markets (Silk Road Marketplace, Agora Market and

Sheep Marketplace). It is unknown if these dark market Bitcoin addresses are for Gill personally or someone else. In addition, approximately 34% of the Bitcoins from Gill's Bitstamp account were transferred to Bitcoin addresses connected with an over-the-counter trading platform called Localbitcoins. Bitstamp contacted Gill about his transactions. Gill stated that he was using his personal Bitstamp account in connection with business / commercial activities connected to his company Bits of 8, LLC. Based on your affiant's training and experience, Gill's transactions from his Bitstamp account have the appearance of an unlicensed money service business.

41. In 2014, Gill also had an account with Coinbase, another cryptocurrency exchange. Coinbase inquired about Gill's account activity because of the large transaction volume that was discovered. Gill told Coinbase, "I am not operating a MSB and I am not registered with FinCEN. I do not transmit money from one person to another, I do not hold funds for customers in depository accounts, nor am I engaged in any other activity which would meet the definition of a MSB according to either US or NC regulations."

42. Records from Gemini Trust, a cryptocurrency exchange, show that Gill deposited approximately $423,670 in cryptocurrency into their exchange in 2018. Part of these deposits were exchanged to United States currency, and then wired to his bank account. He used money in that same bank account to pay for 1105 Park Glen Place, Durham, North Carolina in March 2018.

Debit Cards

43. From 2015 to 2017, documents from Bancorp, a financial institution, identify Gill as owning various debit cards, and that he used over $100,000 in cash to "load" those debit cards. These cards were then used for various withdraws, purchases, or payments made to other credit cards. The following summary shows the volume of funds going into these cards.

Account Number	2015	2016	2017
4420620105919190	$5,875.00		
4565340519378850	$22,265.00		
4565340519338560	$15,735.00	$45,207.14	$11,116.00
479866000003326	$7,260.00		
Total	$51,135.00	$45,207.14	$11,116.00

44. Based upon the above information, your affiant submits there is probable cause to believe that Gill has committed violations of Title 26, U.S.C. Sections 7201 (attempt to evade or defeat a tax) and 7203 (willful failure to file return, supply information, or pay tax), Title 18 U.S.C. Section 1956(a)(3)(B) (money laundering concealment), and Title 18 U.S.C. Section 1960 (unlicensed money service businesses) and that evidence of, fruits of, and property designed, intended, or used in committing, those crimes is located at Gill's residence, in his vehicle, and on his person.

ITEMS TO BE SEIZED

45. By this Affidavit, your affiant is seeking authority to search for any of the records set forth in Attachment A1, B1, and C1. By this Affidavit, your affiant is also seeking authority to search any of the records that may be stored electronically at the premises, vehicle, or person to be searched. The electronic records to be searched and seized are defined in Attachment A1, B1, and C1.

SEIZURE OF EQUIPMENT AND DATA

46. As described above and in Attachments A1, B1, and C1, this application seeks permission to search for records that might be found in whatever form they are found. One form in which the records might be found is data stored on an electronic device or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

47. *Probable cause.* Your affiant submits that if an electronic device or other storage medium is found, there is probable cause to believe those records will be stored on that electronic device or storage medium, for at least the following reasons:

    a. Based on your affiant's knowledge, training, and experience, your affiant knows that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on an electronic device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

    b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage

medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, an electronic device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, electronic storage media—in particular, internal hard drives of computers and other electronic devices—contain electronic evidence of how a device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Users of computers and other electronic devices typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

48. Special Agent-Computer Investigative Specialist (SA-CIS) Rodney Dickerson has informed your affiant that electronic storage medium and computer hardware, software, documentation, passwords, and data security devices may be important to a criminal investigation in four respects, they may: (1) contain contraband, (2) be an instrumentality of

an offense, (3) be fruits of a crime, or (4) contain evidence of crime (items that are evidence or may have been used to collect and store information about crimes) created, stored, or maintained as electronic or digital data/information. Rule 41 of the Federal Rules of Criminal Procedure permits the Government to search for and seize electronic storage medium and computer hardware, software, documentation, passwords, and data security devices which are (1) contraband, (2) instrumentalities, (3) fruits, or (4) evidence of crime. The computer and related electronic storage media can be one or more of the aforementioned classifications.

49. In order to completely and accurately retrieve data maintained in electronic device hardware or on electronic device software, to ensure accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that some electronic device equipment, peripherals, related instructions in the form of manuals and notes as well as the software utilized to operate such electronic device, be seized and subsequently processed by a qualified computer specialist in a laboratory setting. This is true because of the following:

The volume of evidence. Electronic Device storage devices (such as hard disks, cell phones, thumb drives, flash media, tapes, laser disks, CDs, DVDs, etc.) can store the equivalent of hundreds of thousands of pages of information. Additionally, a user may seek to conceal criminal evidence by storing it in random order with deceptive file names. Searching authorities are required to examine all the stored data to determine which particular files is evidence or instrumentalities of

criminal activity. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data analysis on-site.

Technical requirements. Searching computer systems for criminal evidence can be a highly technical process that can require expert skills and a properly controlled environment. The imaging time alone can be significant with larger drives and this would need to be completed before any search would even be attempted to avoid potential data changes, corruption, or loss. It is often difficult to determine the hardware and software used on a system to be searched before the search is executed, and the vast array of computer hardware and software available require even computer experts to specialize in some systems and applications. As a result, it is difficult to know prior to a search: (1) whether a specific expert or search protocol may be required; (2) if so, which expert may be qualified to analyze the system and its data; and (3) whether and what type of controlled environment may be required. Data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Because electronic device evidence can be vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive code imbedded in the system, such as a booby trap), a controlled environment may be necessary to complete an accurate analysis. Further, such searches often require the seizure of most or all of an electronic device's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that, if necessary, a

qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment.

50. Due to the volume of the data at issue and the technical requirements set forth above, it may be necessary that the above referenced equipment, software, data, and related instruction be seized and subsequently processed by a qualified computer specialist in a laboratory setting. Under appropriate circumstances, some types of electronic device equipment can be more readily analyzed and pertinent data seized on-site, thus eliminating the need for its removal from the premises. One factor used in determining whether to analyze an electronic device on-site or to remove it from the premises is whether the electronic device constitutes an instrumentality of an offense and is thus subject to immediate seizure as such--or whether it serves as a mere repository for evidence of a criminal offense. Another determining factor is whether, as a repository for evidence, a particular device can be more readily, quickly, and thus less intrusively, analyzed off-site, with due considerations given to preserving the integrity of the evidence. This, in turn, is often dependent upon the amount of data and number of discrete files or file areas that must be analyzed, and this is frequently dependent upon the particular type of computer hardware involved. As a result, it is ordinarily impossible to appropriately analyze such material without removing it from the location where it is seized.

51. Your affiant recognizes that the location as listed on Attachment A could have unknown companies co-located in the same space, and that a seizure of the electronic devices may have the unintended effect of

limiting the ability to provide service to legitimate customers. In response to these concerns, the agents who execute the search anticipate taking an incremental approach to minimize the inconvenience to legitimate customers and to minimize the need to seize equipment and data.

a. The SA-CIS will attempt to create an electronic "image" of those parts of the electronic devices that are likely to store the things described in the warrant.

b. The government will retain a forensic image of each electronic storage device subjected to analysis for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to questions regarding the corruption of data; establishing the chain of custody of data; refuting claims of fabricating, tampering, or destroying data; and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

c. If imaging proves impractical, or even impossible for technical reasons, then the agents will seize those components of the electronic device system that the agents believe must be seized to permit the agents to locate the things described in the warrant at an off-site location. The seized components will be removed from the premises and returned within three days. If additional time is needed for imaging, agents may request additional time from the Court.

d. If, after inspecting the electronic devices, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it within a reasonable time.

e. With respect to the seizure of electronic storage media or the seizure or imaging of electronically stored information, the search warrant return to the Court will describe the physical storage media that were seized or imaged.

52. Based upon your affiant's consultation with SA-CIS Rodney Dickerson, your affiant is aware that searches and seizures of evidence from electronic devices taken from the premises commonly require agents to seize most or all of a electronic devices input/output peripheral devices, in order for a qualified computer expert to accurately retrieve the system's data in a laboratory or other controlled environment. Therefore, in those instances where electronic devices are removed from the premises, in order to fully retrieve data from an electronic devices system, investigators must seize all the magnetic storage devices as well as the central processing units (CPUs) and applicable keyboards and monitors which are an integral part of the processing unit. It is the Government's intention to first attempt to create electronic copies of the systems on-site if possible or practical. As previously discussed, if creating electronic copies of the systems on-site is not possible or practical, agents will seize the computer hardware and peripherals as necessary to ensure recovery of all the evidence.

53. The analysis of electronically stored data, whether performed on-site or in a laboratory or other controlled environment, may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file directories and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer capable of containing pertinent files, in order to locate the evidence and instrumentalities authorized for seizure by the warrant); opening or reading the first few pages of such files in order to determine their precise contents; scanning storage areas to discover and possibly recover deleted data; scanning storage areas for deliberately hidden files; and performing electronic key-word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

54. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

Unlocking Devices With Biometric Features

55. The warrant your affiant is applying for would permit law enforcement to compel certain individuals to unlock a device subject to seizure pursuant to this warrant using the device's biometric features. Your affiant seeks this authority based on the following:

a. Your affiant knows from training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-

facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In your affiant's training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this affidavit, based on your affiant's training and experience your affiant believes that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. Your affiant also knows from training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. In your affiant's training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in your affiant's training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in your affiant's training and experience, sometimes it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

i. Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant your affiant is applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the premises and reasonably believed by law enforcement to be a user of the device(s), to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face to those same individuals and activate the facial recognition feature; and/or (3) hold the

device(s) found at the premises in front of the face of those same individuals and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

j. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

Conclusion

56. Your affiant has probable cause to believe that evidence and fruits of the crimes of Title 26, U.S.C. Sections 7201 (attempt to evade or defeat a tax) and 7203 (willful failure to file return, supply information, or pay tax), Title 18 U.S.C. Section 1956(a)(3)(B) (money laundering concealment), and Title 18 U.S.C. Section 1960 (unlicensed money service businesses), as well as property designed for use, intended for use, or used in committing those offenses. are:

a) located at Jayton Gill's residence as described in Attachment A with the items to be seized as described in Attachment A1,

b) in his vehicle as described in Attachment B, with the items to be seized as described in Attachment B1, and

c) on his person as described in Attachment C, with items to be seized as described in Attachment C1.

57. Your affiant seeks a warrant for evidence and fruits of criminal violations of Title 26, U.S.C. Sections 7201 and 7203, and Title 18 U.S.C. Sections 1956(a)(3)(B) and 1960, as well as property designed for use, intended for use, or used in committing those offenses.

58. Your affiant believes that Jayton Gill has failed to file personal and business income tax returns as required by federal statute based on the amount of funds he received through his business activities.

59. Your affiant believes that Jayton Gill is evading assessment of his personal income tax liabilities by:

a. Dealing in a cash lifestyle;
b. Using debit cards to hide his personal living expenses; and
c. Concealing his true income by not depositing all cash into his bank accounts

60. Your affiant believes that Jayton Gill is operating an unlicensed MSB and engaging in money laundering by:

a. Acting as a cryptocurrency exchanger
b. Meeting with an FBI UCA to engage in financial transactions
c. Using his bank and cryptocurrency accounts to operate as an unlicensed MSB.

d. Knowingly engaging in financial transactions that are represented as involving proceeds of illegal drug trafficking.

61. Your affiant respectfully submits this Affidavit as probable cause to support the issuance of the requested search warrants.

/s/ Robert Nordlander

Robert Nordlander
Special Agent
Internal Revenue Service
Criminal Investigation

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me via reliable electronic means (telephone), was placed under oath, and attested to the contents of this written affidavit. This the 8th day of February, 2021, at 11:12am.

The Honorable Joe L. Webster
U.S. Magistrate Judge